

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
27 December 2002 (27.12.2002)

PCT

(10) International Publication Number  
**WO 02/103610 A2**

(51) International Patent Classification<sup>7</sup>: **G06J**

(US). **WHITE, Eric** [US/US]; 834 Grant Regency Pointe, Apt. 4-105, Alamonte Springs, FL 32714 (US).

(21) International Application Number: **PCT/US02/16855**

(74) Agents: **BUCZYNSKI, Joseph** et al.; Roylance, Abrams, Berdo & Goodman, L.L.P., 1300 19th Street, N.W., Suite 600, Washington, DC 20036 (US).

(22) International Filing Date: **31 May 2002 (31.05.2002)**

(25) Filing Language: **English**

(81) Designated States (*national*): AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(26) Publication Language: **English**

(30) Priority Data:  
**60/297,769** **14 June 2001 (14.06.2001)** **US**

(71) Applicant (*for all designated States except US*): **MESH-NETWORKS, INC.** [US/US]; 485 North Keller Road, Suite 250, Maitland, FL 32751 (US).

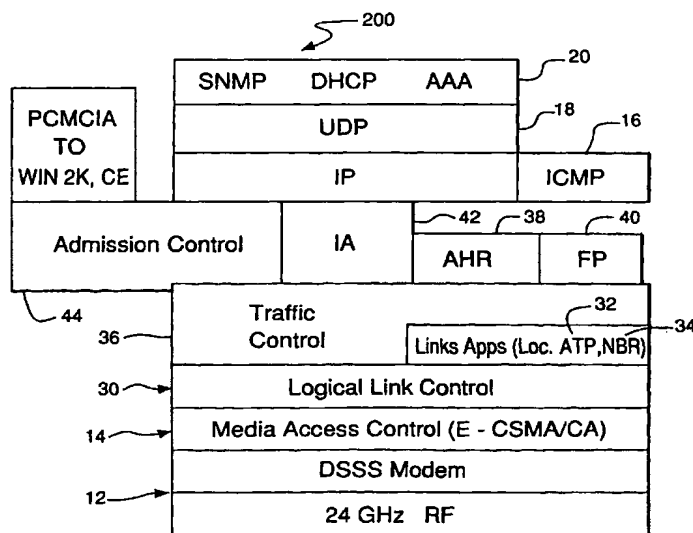
(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR,

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): **WHITEHILL, Eric** [US/US]; 6021 Highgate Place, Fort Wayne, IN 46815

[Continued on next page]

(54) Title: EMBEDDED ROUTING ALGORITHMS UNDER THE INTERNET PROTOCOL ROUTING LAYER OF A SOFTWARE ARCHITECTURE PROTOCOL STACK IN A MOBILE AD-HOC NETWORK



(57) Abstract: A novel software architecture protocol stack with embedded routing algorithms under the Internet Protocol (IP) routing layer in order to provide high quality distribution of multimedia (voice, video, and data) services. These routing algorithms may include Logical Link Control, Adaptive Transmission Protocol, Neighbor Discovery, Traffic Control, Ad-Hoc Routing, Flow Processing, Intelligent Access and Admission Control. These routing algorithms when implemented further provide for advantages in speed of service, reliability of service, self-healing in case of catastrophic failure of an infrastructure component, load-balancing and geographic reuse.



GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

**Published:**

— *without international search report and to be republished upon receipt of that report*

Embedded Routing Algorithms Under the Internet Protocol Routing Layer  
of a Software Architecture Protocol Stack in a Mobile Ad-Hoc Network

BACKGROUND OF THE INVENTION

Field of the Invention:

**[0001]** The present invention relates to a software architecture protocol stack for use in an ad-hoc wireless communication network. More particularly, the present invention relates to a protocol stack having embedded routing algorithms under the Internet Protocol (IP) routing layer, to thus provide high quality distribution of multimedia (voice, video, and data) services in a mobile wireless ad-hoc communications network.

**[0002]** Related subject matter is disclosed in U.S. provisional patent application Serial No. 60/297,769, filed on June 14, 2001, the entire contents being incorporated herein by reference.

- 2 -

Description of the Related Art:

**[0003]** Many different types of wireless communication networks currently exist, such as wireless cellular telephone networks and the like. These types of wireless networks generally employ significant infrastructure, such as base stations, gateways, and so on, that communicate directly with wireless access devices that provide access to services such as the Internet, public switched telephone network (PSTN), and other cellular networks, to name a few. Examples of these types of networks are the current cellular communications networks, such as AMPS, TACS, NMT, GSM, IS-136 and IS-95.

**[0004]** In addition, certain cellular companies have developed networks called Wireless Access Protocol (WAP) networks that are capable of offering data services rather than only voice services. Furthermore, researchers have begun examining the application of ad-hoc networks for the delivery of multi-media content over wireless media. For example, in the Mobile Ad-Hoc Networking Group (MANET) of the Internet Engineering Task Force (IETF), researchers are applying the principles of ad-hoc routing on top of the Internet Protocol (IP), as described in a document by Johnson et al. entitled "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks", in a document by Jacquet et al. entitled "Optimized Link State Routing Protocol", and in a document by Perkins et al. entitled "Ad Hoc On-Demand Distance Vector (AODV) Routing", the entire contents of each of these documents being incorporated herein by reference.

**[0005]** Figure 1 is a conceptual diagram illustrating an example of a protocol stack 10 for a typical IETF-MANET Mobile Ad-Hoc Networking Group. The protocol stack 10 is implemented as a five-layer software stack, referenced from the bottom layer to the top. The lowest layer, the Physical Layer 12, includes the RF and modem circuits involved in generating channel quality information, such as a direct sequence spread spectrum (DSSS) modem with a 2.4 GHz radio frequency (RF) typically associated with code division multiple access (CDMA) systems. The

- 3 -

Physical Layer 12 is responsible for transmitting and receiving configuration and application data with the Network Layer or Media Access Control (MAC) layer 14.

**[0006]** In a typical MANET protocol stack, the MAC layer 14 is specified in the IEEE 802.11 standard for wireless local area networks (LANs) and utilizes a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. As can be appreciated by one skilled in the art, the CSMA/CA protocol may involve initial handshakes of a Request-to-Send (RTS) message followed by a Clear-to-Send (CTS) or Not-Clear-to-Send (NCTS) message exchanged between a source node and a destination node prior to sending the multimedia (voice, video, data) message. Afterward, an Acknowledgement (ACK) message or Non-Acknowledgement (NACK) message may be sent from the destination node to the source node to indicate reception of the transmitted message. Layered above the MAC layer 14 is the routing internet protocol (IP) layer 16, which includes other Internet protocols schemes, such as Internet control message and Internet group management protocol.

**[0007]** In communication with the IP layer 16 is the transport layer 18 that defines the method of communicating. Well-known examples of the transport layer are TCP and UDP protocols. The uppermost layer, which is the application layer 20, provides application protocols, such as dynamic source routing (DSR) or ad-hoc on-demand distance vector routing (AODV) 20a, resource reservation protocol (RSVP) 20b, real time transport protocol (RTP) 20c, simple network management protocol (SNMP) 20d, dynamic host configuration protocol (DHCP) 20e, and authentication authorization and accounting protocol (AAA) 20f.

**[0008]** Although the protocol stack 10 shown in Figure 1 may be suitable for enabling a network to provide multimedia services, such as voice, video and data services, this type of protocol arrangement can be somewhat complex and time-consuming in terms of message delivery time and reliability. Therefore, this protocol stack arrangement has limited capability for commercial applications. Accordingly, a need exists for an improved protocol stack configuration which enables a wireless ad-hoc communication network to deliver multimedia content with sufficient speed and reliability suitable for use in commercial communication networks.

### SUMMARY OF THE INVENTION

**[0009]** An object of the present invention is to provide a protocol stack with embedded routing algorithms under the Internet Protocol (IP) routing layer in a protocol stack used by a wireless mobile ad-hoc communication network.

**[0010]** Another object of the present invention is to employ the use of embedded routing algorithms under the IP routing layer in a protocol stack by an wireless mobile ad-hoc network to enable the network to deliver multimedia content, such as voice, video and data, with optimum speed and reliability.

**[0011]** These and other objects are substantially achieved by providing a protocol stack, adapted for use in a wireless mobile ad-hoc communication network. The protocol stack comprises an Internet Protocol (IP) routing layer, and at least one routing algorithm, embedded in the protocol stack below the IP routing layer, and being adapted to control routing of data packets, including multimedia content, between nodes in the network. The routing algorithm includes at least one of the following layers: Logical Link Control (LLC), Adaptive Transmission Protocol (ATP), Neighbor Discovery (NBR), Traffic Control (TC), Ad-Hoc Routing (AHR), Flow Processing (FP), Intelligent Access (IA), and Admission Control (AC).

**[0012]** These and other objects are also substantially achieved by providing a system and method and for controlling a transmitter, which is adapted for use in a wireless mobile ad-hoc communication network, to transmit at least one packet of information. The system and method employ the operations of identifying a quality of service (QoS) associated with the packet, controlling the transmitter to attempt to transmit the packet to a node in the wireless mobile ad-hoc communication network, and controlling the transmitter to attempt to retransmit the packet to the node in the wireless mobile ad-hoc communication network at at least one period of time from the attempt to transmit based on the QoS associated with the packet, when it is determined that the attempt to transmit the packet to the node has failed. Also, before performing the controlling steps, the system and method can place the packet in a

- 5 -

transmission queue at a position to await transmission based on the QoS associated with the packet, such that a data packet having an associated QoS having a higher value is placed at a position in the transmission queue for transmission ahead of another data packet having another associated QoS having a lower value. Specifically, a data packet containing voice data is placed at a position in the transmission queue for transmission ahead of a data packet containing streaming media, and a data packet containing streaming media is placed at a position in the transmission queue for transmission ahead of a data packet containing non-voice data or non-streaming media data.

**[0013]** These and other objects are further substantially achieved by providing a system and method for controlling a node in a wireless ad-hoc communication network to identify the presence of other nodes in the network. The system and method perform the operations of controlling the node to transmit at least one message to be received by those of the other nodes within a broadcast range of the node, controlling the node to receive responses to the message or messages transmitted by those of the other nodes, determining respective identities of those of the other nodes relative to the node, and at least one route for the node to communicate with another network, based on the responses. The determining operation can determine the respective identities of those of the other nodes based on respective power levels at which the node receives the respective responses, as well as respective locations of those of the other nodes based on the respective responses. Also, at least one of the messages transmitted by the node includes information pertaining to a location of the node and an indication of the suitability of the node to act as a position reference.

**[0014]** In addition, these and other objects are substantially achieved by providing a system and method for routing at least one data packet between a source node and a destination node in a mobile ad-hoc routing network comprising a plurality of nodes. The system and method perform the operation of determining at least one routing path for routing the data packet between the source node and the destination node based on an amount of energy allowed to be expended by the source node to transmit the data

- 6 -

packet, a number of other nodes permitted as hops between the source node and the destination node, an amount of data congestion in an area of the network including the source and destination nodes, and an amount of power remaining in a power source of the source node. The system and method further control the source node to transmit the data packet to the destination node along the determined routing path.

**[0015]** These and other objects are further substantially achieved by providing a system and method for determining at least one route for routing at least one data packet between a source node and a destination node in a mobile ad-hoc communication network comprising a plurality of nodes. The system and method perform the operations of identifying those of the nodes that the source node can use to route the data packet to the destination node based on respective characteristics of the respective nodes, including those of the nodes in a group of available nodes, and determining a route including at least one of the available nodes identified in the identifying step for routing the data packet from the source node to the destination node. The system and method also remove at least one of the nodes from the group of available nodes based on a change in characteristics of at least one of the nodes, or a change in position of the source node, or both.

**[0016]** Each respective characteristic associated with each respective node includes as indication as to whether the respective node is at least one of the following types of nodes: an access node capable of providing the source node access to another network or another portion of the network; a neighboring node of the source node; a neighbor of at least one neighboring node of the source node; a terminal node which is actively a source or sink of data traffic; and a wireless router which is not a neighboring node of the source node. The system and method can therefore include a node in the group of available nodes based on the following priority: an access node having the highest priority, followed by a neighboring node, a neighbor of the neighboring node, a terminal node, and a wireless routing having the lowest priority. Also, the system and method can remove at least one of the nodes based on the following priority: an access node having the lowest priority for removal, followed by



- 7 -

a neighboring node, a neighbor of the neighboring node, a terminal node, and a wireless routing having the highest priority for removal.

**[0017]** The above objects, as well as other objects, can also be substantially achieved by providing a system and method for enabling a node in a wireless ad-hoc communication network to identify an access node via which the node is able to access another network or another portion of the network. The system and method perform the operations of controlling the node to send a message to other nodes in the network, the message including a request for identification of an access node with which the node is associated, and identifying a certain access node as being associated with the node based on information contained in a response message received by the node from the access node. The node can receive the response message that was routed from the access node through at least one of the other nodes. The node can also send at least one data packet to the access node via at least one of the other nodes, for example, as a unicast message.

#### BRIEF DESCRIPTION OF THE DRAWINGS

**[0018]** These and other objects, advantages and novel features of the invention will be more readily appreciated from the following detailed description when read in conjunction with the accompanying drawings, in which:

**[0019]** Figure 1 is a conceptual diagram illustrating an example of a protocol stack for a typical IETF-MANET Mobile Ad-Hoc Networking Group;

**[0020]** Figure 2 is a block diagram of an example of an ad-hoc wireless communications network employing a protocol stack in accordance with an embodiment of the present invention;

**[0021]** Figure 3 is a block diagram of an example of a wireless node as shown in Figure 2;

**[0022]** Figure 4 is a conceptual diagram illustrating an example of a protocol stack in accordance with an embodiment of the present invention, which is adapted for use in a wireless ad-hoc communication network as shown in Figure 2;

- 8 -

**[0023]** Figure 5 is a flowchart illustrating an example of operations performed in relation to the Adaptive Transmission Protocol (ATP) of the protocol stack shown in Figure 4;

**[0024]** Figure 6 is a conceptual diagram illustrating an example of the manner in which the ad-hoc routing capabilities of the network shown in Figure 2 adaptively change routing paths; and

**[0025]** Figure 7 is a timing diagram illustrating an example of the messages sent between the nodes shown in Figure 6.

#### DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

**[0026]** Figure 2 is a conceptual block diagram illustrating an example of a wireless communications network 100 employing an embodiment of the present invention. Specifically, the network 100 can be an ad-hoc packet switched network, which includes a plurality of mobile nodes 102-1 through 102-n (referred to generally as nodes 102 or mobile nodes 102), and a fixed network 104 having a plurality of fixed nodes or access points 106-1, 106-2, ..., 106-n (referred to generally as nodes 106 or fixed nodes 106), for providing the mobile nodes 102 with access to the fixed network 104. A node 102 can be a wireless telephone, radio, user terminal or any other suitable mobile wireless device. The fixed network 104 includes, for example, a core local access network (LAN), and a plurality of servers and gateway routers, to thus provide the mobile nodes 102 with access to other networks, such as the public switched telephone network (PSTN) and the Internet. The network further includes a plurality of wireless routers 107-1, 107-2 through 107-n (referred to generally as nodes 107) which are capable of routing data packets to other nodes 102, 106 or 107.

**[0027]** As shown in Figure 3, each mobile node 102, fixed node 106 or wireless router 107 includes a modem which is essentially a transceiver 108 including a transmitter and a receiver, which collectively can be referred to as a modem, and which are coupled to an antenna 110 and capable of respectively transmitting and receiving signals, such as packetized data signals, under the control of a controller

- 9 -

112. The packetized data signals can include, for example, voice, data or multimedia. Each node 102, 106, 107 further includes a memory 114, which can include a read only memory (ROM) for storing information pertaining to the operation of the node 102, 106, 107 and a random access memory (RAM) for storing information such as routing table information and the like in accordance with which data packets are transmitted, received and routed by the transceiver 108.

**[0028]** Each mobile node 102, fixed node 106 and wireless router 107 can communicate over plural data channels, as well as a reservation channel, using CSMA/CA techniques. An example of a network employing CSMA/CA techniques is described in U.S. patent application Serial No. 09/705,588, the entire contents of which is incorporated herein by reference. In this type of network, a plurality of nodes communicate with each other using plural, shared parallel data channels and a separate reservation channel. As used herein, the term node refers to a communication device operating in a network of communication devices. The node may be a mobile communication device, such as a radio or wireless telephone, or the node may be stationary or fixed in a particular location. Also, as used herein, the term channel refers to a communication path between nodes, and different channels can exist on separate communication media or on a common communication medium, with individual channels being separated by any suitable means, such as time, frequency, or encoding.

**[0029]** Figure 4 is a conceptual diagram of a protocol stack 200 in accordance with an embodiment of the present invention, that is employed in the ad-hoc communication network 100 shown in Figure 2. It is noted that numerals identified in this figure which are identical with those identified in the protocol stack 10 shown in Figure 1 are intended to represent components identical or similar to those shown in Figure 1.

**[0030]** As shown in Figure 4, the protocol stack 200 includes the following protocols: Logical Link Control (LLC) 30, Adaptive Transmission Protocol (ATP) 32, Neighbor Discovery (NBR) 34, Traffic Control (TC) 36, Ad-Hoc Routing (AHR) 38, Flow Processing (FP) 40, Intelligent Access (IA) 42, and Admission Control (AC)

- 10 -

44. The protocol stack 200 also includes the layers 12, 14, 16, 18 and 20 present in the stack 10 shown in Figure 1. As described in more detail below, the protocol stack 200 embeds these protocols and routing algorithms underneath the IP layer 16. The various combinations of these protocol algorithms provide advantages among speed of service, reliability of service, self-healing in case of catastrophic failure of an infrastructure component, load-balancing and geographic reuse when applied to the wireless multimedia delivery of services/messages. These embedded routing algorithms provide high quality distribution of multimedia (voice, video, data) services over mobile multimedia networks that are supported by a significant infrastructure. The infrastructure provides access to services such as the Internet, public switched telephone network (PSTN), and other cellular networks. The embedded routing also enhances the delivery of real time multimedia services over a wide area wireless network where speed and quality of service (QoS) determine the commercial interest in the product offering.

**[0031]** As in the protocol stack 10 shown in Figure 1, the lowest layer in protocol stack 200 is the Physical Layer 12 which, as described above, includes the RF and modem circuits involved in generating channel quality information, such as a direct sequence spread spectrum (DSSS) modem with a 2.4 GHz radio frequency (RF) typically associated with code division multiple access (CDMA) systems. The Physical Layer 12 is responsible for transmitting and receiving configuration and application data with the Network Layer or Media Access Control (MAC) layer 14. As stated, further details of these layers 12 and 14 are described above and will not be further described here.

**[0032]** The next layer in the protocol stack 200 is the Logical Link Control (LLC) layer. The LLC 30 in accordance with an embodiment of the present invention comprises link layer queues, random backoff algorithm, relevancy timers, and retransmission policy which are described in more detail below. These elements combine to insure the reliable and timely delivery of packets across the DSSS modem. The queuing and backoff strategies are Quality of Service (QoS) aware. Specifically, voice packets are transmitted with short backoff timers operating according to a linear

- 11 -

algorithm such that the retransmission attempts are accomplished before the voice segments become irrelevant.

**[0033]** The relevancy timers for voice are set such that the voice segments are successfully transmitted within the jitter buffer expectations of the applications, or they are removed from the queues in favor of transmitting successive voice segments which are relevant to the current playback of the VoIP application. The backoff algorithm for datagrams is based on an exponential algorithm that attempts to reduce congestion by slowing the introduction of data segment onto the channel. The relevancy timers for datagrams are set in accordance with the TCP retransmission timers such that a TCP retry only occurs when it is necessary. Effectively, TCP intervenes whenever the datagram has not been received and all link layer attempts have been attempted without success. A final capability of the LLC 30 algorithm is concatenation of messages to common destinations. This concatenation improves the efficiency of message transfer by using one channel access attempt to transfer up to ten messages. The LLC 30 queues a small number of packets greater than one to support concatenation as well as the ability to send packets to nodes that are currently free when the packet at the front of the queue is addressed to a node that is currently busy.

**[0034]** The queues, random backoff algorithm, relevancy timers, and retransmission policy of the LLC layer 30 will now be described in more detail.

**[0035]** Queues – The link layer queuing algorithm is a prioritized First-In-First-Out (FIFO) algorithm. The priority scheme for this queue is dependent on the Quality-of-Service(QoS) requested and, secondarily, on the number of transmission attempts already accomplished. The QoS is based on the IP TOS field in the IPv4 or IPv6 header. Within this field, the precedence values are used to order the packets in the LLC queue. Within a precedence value, packets are ordered according to the number of transmission attempts where those packets which have been attempted are sent prior to those which are new arrivals to the queue. This promotes the correct ordering of the packets which is beneficial to some applications, such as Microsoft NetMeeting. If the IP TOS field has not been set appropriately, the network 100

determines the type of application which generated the datagram. Datagrams are identified as Network Control, Voice, Streaming Media, and Data at a minimum.

**[0036]** Random Backoff – The random backoff algorithm is dependent on the QoS requested. Within the network 100, datagrams are marked according to their application if the IP TOS field has not been set appropriate. Datagrams that are marked as Voice or Streaming Media employ a linear random backoff algorithm according to the following equation:

$$\text{RandomBackoff} = \text{MIN\_BACKOFF} + \text{random}(\text{REAL\_TIME\_BACKOFF\_INTERVAL})$$

**[0037]** The MIN\_BACKOFF value is currently set to 5 milliseconds. The value of REAL\_TIME\_BACKOFF\_INTERVAL is currently set to 10 milliseconds. This creates a uniformly distributed random interval between 5 and 15 milliseconds. The linear backoff algorithm insures that time sensitive datagrams (Voice, Streaming Media) are not subjected to the congestion control function which is inherent in exponential backoff algorithms. That is, time sensitive datagrams should be delivered quickly or not delivered at all. Time sensitive datagrams which arrive late to the destination application are destroyed without entering the video or audio codec's, and thus, they are better off not transmitted.

**[0038]** Non-real time datagrams are employ an exponential backoff algorithm according to the following equation:

$$\text{Random Backoff} = 20 + \text{Random}(100) * 2^{(\text{Number of failed attempts})} \text{ms}$$

**[0039]** The exponential term in the random backoff algorithm progressively increases the amount of time a datagram is held from the channel. This mechanism responds to perceived congestion on the reservation channel by slowing down this nodes contribution to the problem. Datagrams undergoing longer random backoff intervals have additional time to learn about the current channel conditions and take appropriate action to improve their probability of successful delivery.

- 13 -

**[0040]** Relevancy Timers – The link layer queuing algorithm has been augmented with a relevancy timer for datagrams to reduce the amount of bandwidth that is wasted due to exceeding its lifetime. Datagrams which have exceeded their relevancy timer are discarded and the traffic control module is notified so that additional datagrams can be considered for transmission by the logical link control module. The relevancy timers are set to the following exemplary values depending on their datagram type, although any suitable values can be chosen:

Voice = 50ms  
Streaming Media = 100ms  
Data = 1 second

**[0041]** The Voice and Streaming Media timers are associated with delivering an audio stream which meets the recommendations of the ITU. The data timer is set to 1 second to interoperate with the TCP protocol. TCP has a timeout mechanism for segment retransmissions when acknowledgements are not received in the proper time. The protocol stack seeks to minimize the duplicate delivery of TCP segments caused by data arriving late due to a transient condition on congestion.

**[0042]** Retransmission policy – The number of transmission attempts are dependent on the data type being forwarded. Voice and Streaming Media are limited to four channel access attempts due to their relevancy. Datagrams are permitted up to six channel access attempts to improve link layer reliability and minimize TCP retransmissions.

**[0043]** As shown in Figure 4, the next layer in the protocol stack 200, which is identified as the Link Apps layer, includes the Adaptive Transmission Protocol (ATP). The ATP 32 algorithm shown is integrated with the backoff strategy in the LLC and the signal quality extracted from the DSSS Modem. The ATP 32 algorithm optimally chooses the next data rate (currently adjustable between 500 Kbps and 8 Mbps) and the next power level (currently adjustable between -10 Dbm and +30 Dbm). This algorithm attempts to adjust the transmission parameters such that the

- 14 -

maximum data rate is used to avoid congestion subject to maintaining a high probability that the message transfer will succeed.

**[0044]** In the discussion that follows, the source node (e.g., node 102, 106 or 107 in Figure 3) is defined to be the source of the transmission, not necessarily the source of the packet. Similarly, the destination node (e.g., node 102, 106 or 1070 is defined to be the destination for the transmission, not necessarily the final destination for the packet. The destination node is assumed to be within communication range of the source node. The transmission parameters include the information rate and transmitter power level to be used for a transmission. The ATP utilizes measurements made in the destination node's receiver to optimize the transmission parameters for subsequent packet transmissions. The channel quality measurements are made during the reception, demodulation, and decoding of the message packet.

**[0045]** The channel quality statistics include the bit-error rate (BER) estimate, the number of multipath signals present during demodulation, the post-detection signal quality (PDSQ), and the analog gain control (AGC) output. The BER estimate is based on the ratio of bit errors to packet length. The bit error count is obtained by encoding the decoder output symbols and comparing this sequence to the sequence of hard decisions made on the input symbols of the decoder. The error count is the number of symbol positions in which these two sequences differ. The BER is used in estimating the severity of interference or path loss affecting the communication link between the source node and the destination node. The number of multipath signals is estimated by the counting the number of taps employed by the RAKE processor within the DSSS modem. The number of multipath signals is used in estimating the link margin and the severity of the multipath. The PDSQ is obtained from the outputs of the correlator during demodulation and is used in estimating the link margin and the severity of the multipath or other interference. The AGC system is used in estimating the total power of the received signal and the resulting link margin.

**[0046]** In this example, each node in the network maintains one table, an ATP-table, for each neighbor. In the ATP-table, the node stores the information rate and power information to be used for transmission of message packets to the



- 15 -

corresponding neighbor. The ATP-table in this example contains 4 arrays which store the PDSQ, BER, AGC, and number of multipath signals tracked for the last N completed transmission attempts to the corresponding neighbor. A completed transmission attempt is a transmission attempt for which an acknowledgement (ACK) or negative acknowledgement (NACK) has been received by the source node. The ATP-table also maintains the message success status for the last N completed transmission attempts and the time at which the channel quality information is stored.

**[0047]** An example of the details of the ATP are illustrated in the flowchart of Figure 5.

**[0048]** If the source node has a packet to send, in step 1000, it first sends to the destination node an RTS packet containing the information rate and power information from its ATP-table for the destination node. The proposed values are based on channel quality measurements included in the ACKs and NACKs resulting from N previous completed transmission attempts. If more than T seconds have elapsed since the last ACK or NACK was received, the available channel quality measurements from the previous transmission attempts are considered out-of-date and are discarded. If no channel quality information is available, the node proposes a set of default parameters, e.g. maximum power and low information rate. Also, a different set of default parameters can be chosen so as not to cause an immediate congestion problem.

**[0049]** The ATP 32 allows the destination node to make a correction to the transmitter power level if there has been a significant change in the path loss or the interference conditions since the last packet transmission occurred. If the destination node accepts the RTS packet, it employs the RTS channel quality measurements, the RTS transmission power level, and the source's requested information rate to propose a power level to be used in the transmission of the packet on the communication channel between the two nodes. In determining its proposed power level, the destination also accounts for possible differences in fading and interference between the reservation channel and the communication channel. If the destination node's calculations indicate that, for the proposed information rate and maximum transmit

- 16 -

power, the message packet will not be successfully received, then a negative CTS (NCTS) packet is sent to the source node in step 1010. In the event that a NCTS is received by the source node, the source node updates its ATP-table for the corresponding neighbor and determines in step 1020 whether there is an insufficient link margin. If there is an insufficient link margin, the transmitter power level is set to max power in step 1025, and the information rate is decremented by one level if possible. That is, it is not possible to decrement the information rate if the setting is already at the minimum information rate. On the other hand, if there is not an insufficient link margin, then no change occurs in the transmitter power level and the information rate.

**[0050]** However, in the event that the destination node's calculations indicate that it is okay to send the packet, the destination node sends to the source node a CTS packet containing its suggested power level. The source node confirms whether the CTS packet was received in step 1030. If not, the process proceeds to step 1040, and no change occurs in the transmitter power level or information rate. Specifically, the ATP algorithm makes note of the lack of response to an RTS. Initially, it assumes that the missed CTS is due to the destination node being on a data channel as opposed to the destination node moving out of range. After multiple missed CTS's, the ATP algorithm will declare the destination node as lost which will cause the routing algorithms to determine an alternate path to the final destination. Upon receiving the CTS in step 1030, the source node compares the destination suggested power level to its proposed power level stored in the ATP-table for the corresponding neighbor. Although it is possible that the destination node propose a lower power level than the source node, the ATP in this example will only allow the destination node to increase the transmitter power level. The decision to decrease the power level will be based only on the more reliable statistics measured on the communication channel. Thus, the message packet is transmitted at the higher of the source-suggested power and the destination-suggested power. The information rate will be that which is proposed by the source node. The destination node is not permitted to request a lower data rate as this may violate the expectations of the QoS algorithms. Likewise, the destination

- 17 -

node is not permitted to request a higher data rate as the source node may have determined that the higher rate does not meet the reliability requirements.

**[0051]** Upon receiving the message packet, the destination node measures the PDSQ, BER, AGC, and number of multipath signals present during demodulation. If the packet decodes successfully, the destination node sends the channel quality information to the source in an ACK packet. If the packet does not decode successfully, the destination node sends the channel quality information to the source node in a NACK packet.

**[0052]** After successful decoding of an ACK or NACK packet, the source node learns the values of the channel quality information. This channel quality information and the time at which it is received is stored in the ATP-table. If an ACK is received, the message is considered successful; otherwise the message is considered unsuccessful. The success status is also recorded in the ATP-table. Each channel quality measure, combined with the available channel quality history, is compared against a set of thresholds. Based on these thresholds and on the previous transmission parameters, the source node proposes a power level and information rate for the next transmission to the neighbor of interest. The proposed transmission parameters are stored in the ATP-table for use in transmitting the next packet addressed to that destination node.

**[0053]** That is, as shown in Figure 5, if the source node determines in step 1060 that no ACK or NACK has been received, the operations proceed to step 1070 where the source node determines if the previous ACKs or NACKs have been received. If so, no change occurs as indicated in step 1080. However, if the previous ACKs or NACKs have not been received, the process proceeds to step 1090 where the power level of the transmitter in the source node is increased by one step if possible. If this is not possible, the information rate is decreased by one step.

**[0054]** If, however, the source node determines in step 1060 that an ACK or NACK has been received, the process proceeds to step 1100 where the source node determines if the packet is correct. If the packet is not correct, the process proceeds to step 1110 where the source node determines whether the bit error rate (BER) is less

- 18 -

than a certain value  $b_2(r)$ . That is, as will now be explained, the process generally operates on the principle that if the BER of the presently received message is slightly bad and the BERs of previous "m" number of messages were fine, then no change is made to the transmission power or information rate. The value "m" can be, for example, 3 or any other suitable number, meaning that the process will not change the transmission power or information rate if only two of the previous messages had BERs which were marginally unacceptable. However, once 3 received messages in a row have BERs which are marginally unacceptable, the algorithm either lowers the information rate at which the next transmission occurs, or increases the power at which the next transmission occurs.

**[0055]** Accordingly, if the BER of the message is less than the value  $b_2(r)$ , the process proceeds to step 1120 where it is determined whether the previous "m" packets have been received correctly. If so, no change in transmission power or information rate occurs as indicated in step 1130. However, if those packets have not been received correctly, the process proceeds to step 1140 where the source node calculates the link margin. Likewise, if the BER is determined to be equal to or greater than the value  $b_2(r)$  in step 1110, the process proceeds directly to step 1140 where the link margin is calculated.

**[0056]** In step 1150, the link margin (LM) is compared to the increasing energy link margin  $L_1$ . If LM is greater than or equal to  $L_1$ , the process proceeds to step 1160 where it is determined whether the last  $n_3$  divided by  $m_3$  BERs are less than the value  $b_2(r)$ . In these two steps, the algorithm is determining whether this is a temporary or longer lasting condition. If the link margin was acceptable ( $>L_1$ ), this transmission failed due to a burst interference of some type which is unlikely to recur and is not indicative of current conditions. However, if this condition occurred a significant number of times ( $n_3$ ) within the last  $m_3$  transmissions, it is a condition which the algorithm will attempt to overcome by increasing signal energy, either by transmitting at a lower information rate or at a higher power. Accordingly, if it is determined in step 1160 that the last  $n_3$  out of  $m_3$  messages were successfully received, that is, had a BER less than the value  $b_2(r)$ , there is no change as indicated in step 1170. If not,

- 19 -

the source node in step 1180 decreases the information rate by a single increment, if possible, and increases the transmission power by one increment if possible.

**[0057]** However, if in step 1150, LM is determined to be less than  $L_1$ , the process proceeds to step 1190 where the source node determines whether the number of transmission paths combined within the RAKE (DSSS) receiver is less than or equal to a value K. If so, the source node believes that the signal problem is NOT multipath related and in step 1200 increases the transmission power by  $(L_1 - LM)$  if possible, or decreases the information rate by  $(L_1 - LM - \text{power increase})$ . Specifically, the algorithm attempts to add enough signal energy to overcome the deficit in link margin, which can be done by increasing transmission power and decreasing the information rate. In this case, the algorithm attempts to overcome the deficit with transmission power first, and information rate second. However, the algorithm can instead decrease data rate first, and then increase transmission power second. Accordingly, if the number of transmission paths combined within the RAKE (DSSS) receiver is not less than or equal to a value K, the source node believes that a multipath condition exists and in step 1210, decreases the information rate by  $(L_1 - LM)$  if possible, or increases the transmission power by  $(L_1 - LM - \text{information rate decrease})$ .

**[0058]** It should also be noted that multipath conditions are more receptive to increases in signal energy brought about by changes in the information rate rather than increases in power. An increase in power simply increases the level of multipath interference relative to the increase in the signal paths which are being used by the rake modem. Power increases do not change the ratios between good signal and destructive multipath. On the other hand, a decrease in the information rate frequently converts the multipath interference into energy which can be combined into the good signal monitored by the RAKE receiver in the DSSS modem.

**[0059]** As indicated in the flowchart and as explained above, steps 1110 through 1210 can occur if the source node determines in step 1100 that the packet is not correct. However, if the packet is correct, the process proceeds to step 1220 where the source node determines whether the BER is less than the value  $b_1(r)$ . If not, the

- 20 -

source node calculates the link margin LM in step 1230. As will now be explained, in this case, although the packet was received correctly, the link margin is indicating that a problem with reception is likely to occur shortly. This sequence of steps attempts to proactively adjust the signal energy prior to detection of a problem by the failed message method described above.

**[0060]** The source node then determines in step 1240 if the LM is greater than or equal to  $L_1$ . If not, the source node determines whether the number of transmission paths is less than the value K in step 1250. If so, the source node in step 1260 increases the transmission power by  $(L_1 - LM)$  if possible, or decreases the information rate by  $(L_1 - LM - \text{power increase})$ . If not, the source node in step 1270 decreases the information rate by  $(L_1 - LM)$  if possible, or increases the transmission power by  $(L_1 - LM - \text{information rate decrease})$ . These operations are similar to the corresponding operations discussed above.

**[0061]** However, if the source node determines in step 1240 that the LM is greater than  $L_1$ , the source node determines in step 1280 whether the last  $n_4$  divided by  $m_4$  BERs are less than the value  $b_1(r)$ . If so, there is no change as indicated in step 1290. If not, the source node in step 1300 decreases the information rate by a single increment, if possible, and increases the transmission power by one increment if possible. In this latter case, the source node has determined that, although the link margin is sufficient, the bit error rate continues to be marginal and is likely to result in a failed transmission attempt within the next few packets. A proactive step to increase signal energy is likely to be needed to maintain a reliable link.

**[0062]** Concerning step 1220 again, if the source node determines that the BER is less than or equal to the value  $b_1(r)$ , the process proceeds to step 1310 where the source node determines if the previous  $m_2$  packets are correct. If not, there is no change as indicated in step 1320. However, if the packets are correct, the source node calculates LM in step 1330 and determines if LM is greater than or equal to a value  $L_2$  in step 1340. If not, there is no change as indicated in step 1350. However, if so, then the source node determines whether the number of transmission paths is less than or equal to 1 in step 1360. If the number of paths is less than or equal to 1, the source

- 21 -

node in step 1370 increases the information rate by one step if possible or decreases the transmission power by one step if possible. However, if the number of paths is greater than 1, the source node increases the information rate by one step if possible, or decreases the power by one increment if possible. In this sequence of steps, the ATP algorithm is verifying that the link is reliable and has been reliable for several previous transmissions before reducing the transmitted signal energy. Reducing the transmitted signal energy has the benefits of either transmitting the datagram faster (reduced delay, increased network throughput) or using less power (longer battery life and increased geographic reuse of frequency).

**[0063]** As further shown in Figure 4, the layer of the protocol stack 200 that includes the ATP 32 also includes the Neighbor Discovery (NBR) algorithm 34. The NBR 34 serves two purposes: rapid discovery of infrastructure and neighborhood size maintenance. The NBR algorithm 34 uses a solicitation message to discover pieces of infrastructure that are used to initialize the device and connect it to the rest of the world, such as the Internet, PSTN, other cellular networks, and so on. The NBR algorithm 34 also sends out beacons at a slow rate to probe the neighborhood. By maintaining a reasonable size neighborhood, maximal geographic reuse can be obtained. The NBR algorithm 34 attempts to maintain a neighborhood consisting of less than twenty nodes such that no one at the fringes is denied service. Nodes at distance are expected to use the store and forward techniques of ad-hoc routing whenever possible to avoid high power transmissions which block large geographic areas.

**[0064]** Furthermore, the NBR algorithm relies on passive listening for much of its information. The media access control algorithm forwards all received RTS/CTS exchanges along with the received signal strength indicator to the NBR algorithm 34. The NBR algorithm 34 uses the received power to maintain knowledge about the neighborhood in terms of neighbor identities, received power, data rates to destinations, and limited connectivity information. The connectivity information includes both the source address (node which made the transmission) as well as the destination address. Destination addresses that are also neighbors make up the

- 22 -

immediate neighborhood. Destination addresses that are not currently neighbors are elements of the neighbors neighbor list. The neighbor's neighbor list is used to gauge the connectivity of this nodes neighborhood. A strongly connected network has a large list of neighbors and a smaller list of nodes at two hops. On the contrary, a weakly connected network has a small list of neighbors relative to the list of nodes at two hops. This information may be used for modification of the transmission policy by the media access control algorithm. Strongly connected networks exhibit less of the near/far CSMA problem than weakly connected networks. The media access transmission policy can be more aggressive in its use of channel resources than the weakly connected network.

**[0065]** Additionally, the neighbor discovery advertisement has been extended to include the node's position and an indication of it's suitability to act as a position reference. Wireless routers (WR) 107 and Intelligent Access Points (IAP) 106 (see Figure 2) are generally preferred as position reference as they are typically installed in a fixed location and given an accurate position.

**[0066]** As further indicated, the Link Apps layer includes a location (LOC) application. The location application issues requests for range measurements to the media access control algorithm. The location application maintains a list of nodes, typically WR's and IAP's, which have a known location. The location application selects a minimum of four nodes and requests range measurements. As the measurements complete, they are forwarded from the MAC to the LOC. Once the LOC obtains the expected measurements, the position determination algorithm calculates the position of the mobile node. This calculation is available to the host computer for use in any location related applications such as tracking, locality of services (nearest Italian restaurant with three stars), or location dependent advertising. An example of the operations performed by the LOC application are set forth in U.S. Patent Application Serial No. 09/973,799 of Eric A. Whitehill, filed on October 11, 2001 and entitled "System and Method for Efficiently Performing Two-Way Ranging to Determine the Location of a Wireless Node in a Communication Network", in U.S. Patent Application Serial No. 09/996,603 of John M. Belcea, filed on November 30,



- 23 -

2001 and entitled "A System and Method for Computing the Signal Propagation Time and the Clock Correction for Mobile Stations in a Wireless Network", and in U.S. Patent Application Serial No. 09/988,001 of John M. Belcea, filed on November 16, 2001 and entitled "A System and Method for Computing the Location of a Mobile Terminal in a Wireless Communications Network", the entire contents of each of these applications being incorporated herein by reference.

**[0067]** The next layer in the protocol stack 200 is the Traffic Control (TC) layer 36. The TC 36 process operates similarly to the LLC 30 in terms of queuing algorithms according to Quality of Service requests and relevancy. All discussions in the LLC 30 relative to these two subjects are equally applicable to TC 36 and thus will not be repeated here. The TC 36 algorithm holds the majority of transmission packets until they are ready to be serviced by the LLC 30. The TC 36 holds onto the packet so that the routing decision is made at the last time interval without affecting the high-speed interaction between the LLC 30 and the MAC.

**[0068]** The next layer in the protocol stack 200 is the Ad Hoc Routing (AHR) layer 38. As can be appreciated by one skilled in the art, the AHR 38 strategy is a least cost type routing algorithm where the cost is a algebraic expression containing the routing metrics: energy, hops, congestion, and battery life. These metrics are used to determine which route is optimal given the QoS requirements of the given traffic type. Embedding of the AHR algorithm 38 beneath the IP layer 16 as in the embodiment of the present invention shown in Figure 4 preserves the real time nature of the traffic that is transiting the network. This is contrary to the execution of the routing algorithms above the IP layer 16, as in the conventional stack shown in Figure 1, which requires every packet to transit the IP layer 16 with its associated queuing and processing delays. These hindrances in performance are created by the use of a general protocol that is not tailored to the real time requirements of traffic such as voice. Embedding only the required functionality beneath the IP layer 16 and tailoring the interrupt structure of the real time operating system results in superior performance.

- 24 -

**[0069]** As can be further appreciated by one skilled in the art, the AHR algorithm 38 is a modified distance vector algorithm. The modifications to the distance vector algorithm include maintaining one primary and two backup routes; cost metric which is a function of energy, hops, congestion, and battery; on-demand elements to inform active traffic streams of link failures or local repairs; pre-emptive handover support to the IAP association algorithm; and selective pruning to reduce size in bytes of routing advertisement. In this example, this algorithm maintains three current routes to each destination. Routes are maintained by the Adaptive Transmission Protocol for next hop data rates/power. Routing Updates are used for destinations not reachable with one transmission in addition to exchange of the battery and power metrics.

**[0070]** It is also noted that the pruning algorithm can add nodes to the routing algorithm according to the following rules:

1. IAP's
2. Neighbor nodes (especially wireless routers)
3. Neighbor's neighbors
4. Other terminal nodes – typically, this would include nodes which are actively sources or sinks of traffic
5. Wireless routers which are not neighbors – WR's which are not neighbors are included on a space available basis. WR's are not destinations of traffic from within the Ad-Hoc network. Rather, they are only destinations of Network Management type traffic from an IAP which maintains the route. Wireless routers are implicitly included by examining the cost metrics to other destinations advertised by nodes in category 2 whose routes likely include a wireless router.

**[0071]** Furthermore, the On-Demand elements are used to inform active traffic streams of link failures or local repairs. These elements are accomplished with a unicast message entitled "Instant Routing Update (IRU)". As these messages are sent unicast with high priority, they can quickly and reliably inform nodes that a link has broken. As the IRU's are forwarded toward the original source, relaying nodes can

- 25 -

make alternate choices of forwarding node to repair the traffic flow, as shown in Figures 6 and 7.

**[0072]** That is, if node Z is sending packets to node D along the path A-B-D and the link between nodes B and D fails, node A can adaptively begin sending the packets along the path A-C-D. As shown in Figure 7, node Z sends a datagram "n" to node A, which sends the datagram "n" to node B. When the link between nodes B and D fails, node B provides an instant routing update to node A indicating the failure. When node Z sends the next datagram "n+1" to node A, node A will send that datagram to node C, which will then send the datagram to node D. When the link between nodes B and D ultimately recovers, node B sends an instant routing update to node A indicating that the route is again available. Based on the conditions of the route along path A-B-D versus path A-C-D, node A can choose to remain sending packets along path A-C-D, or switch back to path A-B-D.

**[0073]** The Ad-Hoc routing algorithm also depends on the passive listening feature of the neighbor discovery algorithm. As described above, the NBR algorithm 34 continuously extracts from all received RTS/CTS messages the power and data rates of connections between neighbors and other nodes which may or may not be this neighbor's nodes. The NBR algorithm 34 has the ability to invalidate nodes which have not been heard from in too long a time. These invalidations are presented to the routing algorithm so that nodes which are no longer available are removed from the forwarding table within the routing algorithm.

**[0074]** The next layer in the protocol stack 200 is the Flow Processing (FP) layer 40. The FP algorithm 40 performs functions similar to the RSVP 20b protocol within the IP stack 10 shown in Figure 1. The FP 40 solution has the same advantages in terms of embedding the solution for greater speed and reliability for delivery of real time traffic. FP 40 works by negotiating a source routed path from source to destination where the intermediate relayers agree to allocate some portion of their bandwidth for the FP 40 request that has been requested. In this way, relayers as well as the destination have effectively signed contracts agreeing to deliver the messages within the requirements of the traffic type (i.e. delay, throughput, and reliability).

- 26 -

This is accomplished by permitting intermediate nodes to prioritize the contracted traffic such that this traffic is served before best effort traffic. Additionally, the intermediate relayers have the ability to reject lower priority datagrams when they are expecting to receive traffic that has been contracted.

**[0075]** The next layer in the protocol stack 200 is the Intelligent Access (IA) module 42. The IA module 42 is the embedded module that creates an association between a subscriber device and an Intelligent Access Point (IAP). The IAP provides the interface between the wireless and the wired assets. The IAP permits the wireless user to access all types of services such as the internet, public telephone network, and cellular network. The embedding of the IA 42 module permits the user to quickly associate, authorize, and authenticate itself within the network. Once these processes are complete, the user has full access to all of the services provided. Typical cellular devices require upwards of ten seconds to accomplish these functions, where a similar set of actions using this embodiment of the present invention may be accomplished within two seconds. The IA 42 algorithm also supports the handoff of subscriber devices between different IAPs. As users migrate within a metropolitan size area, the IA 42 algorithm determines when it is appropriate to create a new association rather than rely on the multi-hop characteristics of the ad-hoc protocol. In general, shorter paths to the IAPs are preferable.

**[0076]** The next layer in the stack 200 is the Admission Control (AC) layer 44. The AC 44 process serves several functions. In general, ad-hoc networks attempt to avoid global broadcasts. These broadcasts are typically associated with internet protocols such as DHCP. DHCP issues a broadcast to locate a DHCP server from which an IP address is obtained. Although a broadcast could be performed in an ad-hoc network via a flooding approach, these techniques are very painful in terms of bandwidth required to reach all nodes within the network. The AC 44 module traps the DHCP broadcasts and tunnels requests to an IAP that performs a broadcast on the wired media where the DHCP server resides. In this way, the DHCP request is turned into a unicast transfer between known entities. Unicast transfers are much more reliable and efficient than the broadcast mechanism.

- 27 -

**[0077]** Another element of the AC 44 protocol is the throttling of data into the network. The AC 44 module determines the quality of service required and responds appropriately based on the current network conditions as determined by the routing protocol. For example, voice messages may be entered into the protocol stack without delay while datagrams may be held for a short time. Delaying datagrams effectively causes the TCP protocol to throttle back its estimate of the network congestion and the TCP protocol will enter traffic into the network at a slower pace. This throttling action allows the underlying network to reliably deliver the data without compromising the ability of the network to deliver the quality of service required by real time applications.

**[0078]** As mentioned above Speed of Service; Reliability of service; Self-Healing in case of catastrophic failure of an infrastructure component; Load-Balancing and Geographic Reuse are all increased by the protocol stack 200 according the embodiment of the present invention described above. Speed of service is provided by the distributed pooling of information regarding the network operation at all nodes within the network. Through the exchange of ad-hoc routing updates as well as flow processing bandwidth guarantees, nodes are advised of the route which best meets their quality of service requirements. In the case of voice, speed of service is critical. Through the use of redundant paths, voice messages are forwarded to their destination along the paths that exhibit the shortest delay with sufficient reliability. The combination of optimal paths with bandwidth reservations according to this embodiment insures that voice traffic is delivered within the 150 ms recommendation by the International Telecommunications Union (ITU).

**[0079]** Furthermore, the reliability of service through reliable delivery of IP datagrams over ad-hoc wireless networks is improved with the use of embedded techniques described above, which combines point-to-point and end-to-end features whose sum provides the required reliability. Typical wireless networks, such as 802.11 networks, may use link layer protocols to perform retransmissions if the transmission is found to be in error. In the case of 802.11, the use of an acknowledgment of successful transmission is an option. In the strategy according to

- 28 -

the described embodiment of the present invention, the link layer retransmission strategy with full acknowledgment is coupled with the self-leveling and bandwidth guarantees provided by the ad-hoc routing protocols.

**[0080]** Full acknowledgment permits a rapid retransmission, which benefits both speed of service and reliability. In the case of the retransmission attempts, the adaptive transmission protocol benefits from the signal quality information returned by this acknowledgment, and can take appropriate actions such as increasing power and lowering data rate to improve the signal to noise ratio and insure a reliable transmission. One typical cause of reliability loss in other networks is the overload of traffic over particular routers. Once other routers get overloaded, they discard packets as their queues have over-filled. The ad-hoc routing technology according to the embodiment of the present invention described above avoids this problem through the self-leveling property. Within the routing algorithm, a congestion metric is distributed which informs upstream nodes of congested conditions and permits them to choose alternate routes which avoid overloaded nodes. Also, the bandwidth guarantees provided within the embedded software force the traffic which can cause an overload away from nodes which have signed contracts to provide high quality service such as voice.

**[0081]** As can be further appreciated by one skilled in the art, Ad-Hoc networks have a natural property that provides an advantage over traditional cellular and 802.11 implementations. In cellular networks, a base station or pico-cell is used to gather all traffic within a geographic area and forward it to the correct endpoint. In case of a catastrophic failure of an infrastructure component (lightning, power outage,) subscribers are unable to complete their calls within the coverage area of the stricken cell. In ad-hoc networks, the outage is identified by the subscribers and their calls are immediately re-routed to other wireless to wired transitions points (Intelligent Access Points in present invention). In ad-hoc networks, it is unlikely that a call will be dropped and service will be maintained to all subscribers wishing to make calls after the catastrophic failure has occurred. In cellular networks, the calls are dropped and service is impossible until the failure has been remedied through equipment

- 29 -

replacement or a redundant unit is brought on-line. The cellular solution is both expensive and provides inferior service to the customer.

**[0082]** Furthermore, in cellular networks, it is relatively easy to demonstrate a situation where service is not obtainable due to an overload of customers attempting to make calls. Typical examples of this are the arrival of an airplane or flight cancellations in an airport, halftime at a football game, and a conference during a break period. Cellular phones contact the nearest cellular station and once it's capacity is full, additional calls are denied. In ad-hoc networks, the routing algorithms balance the peak demand by routing some calls to IAP's that are further away from the user. In the football example, calls may be directed to the IAP's in adjacent buildings by wireless routers on the roof of the stadium. The multiple hops required to redirect the call to IAP's at greater distances are accomplished well within the delay budget required for acceptable delay. The property of load balancing permits a much greater number of users concentrated in dense area to complete their transactions. Load balancing is accomplished on an end-to-end basis by the routing metrics and the bandwidth reservations portion of the present invention ad-hoc routing strategy.

**[0083]** Also, cellular networks provide coverage over a specified geographic interval. All calls are routed between the user and the base station or pico-cell. Thus, the central point (base station/pico cell) becomes the bottleneck that limits the call volume. In the present invention solution, all nodes (subscriber devices, wireless routers, and IAP's) are a part of the network and may be used to relay/route calls. Ad-hoc technologies get greater geographic reuse due to the aggressive use of power control to permit frequency reuse that is dependent on the density of users. As the geographic area becomes more dense, the algorithms reduce the transmit power which blocks a small geographic area. By creating smaller blocked areas, multiple transmissions may be accomplished in parallel. This provides an increase in the volume of calls that can be accomplished. Cellular companies are limited to a fixed power setting surrounding their pico-cell. All transmissions by the pico-cell/base station necessarily block the entire geographic area. By transmitting the minimum

- 30 -

required transmit power, the techniques provided by the embodiment of the present invention described above permits multiple simultaneous transmission to be accomplished.

**[0084]** Other variations of the embodiment described above may also be employed in the network 100. For example, the routing protocols discussed above currently are based on a distance vector approach. Alternatively, Link-State and On-demand approaches are equally admissible within this protocol architecture with similar benefits.

**[0085]** Although only a few exemplary embodiments of the present invention have been described in detail above, those skilled in the art will readily appreciate that many modifications are possible in the exemplary embodiments without materially departing from the novel teachings and advantages of this invention. Accordingly, all such modifications are intended to be included within the scope of this invention as defined in the following claims.



What is claimed is:

1. A method for controlling a transmitter, which is adapted for use in a wireless mobile ad-hoc communication network, to transmit at least one packet of information, the method comprising:

identifying a quality of service (QoS) associated with said packet;

controlling said transmitter to attempt to transmit said packet to a node in said wireless mobile ad-hoc communication network; and

controlling said transmitter to attempt to retransmit said packet to said node in said wireless mobile ad-hoc communication network at at least one period of time from said attempt to transmit based on said QoS associated with said packet, when it is determined that said attempt to transmit said packet to said node has failed.

2. A method as claimed in claim 1, further comprising:

before performing said controlling steps, placing said packet in a transmission queue at a position to await transmission based on said QoS associated with said packet.

3. A method as claimed in claim 2, wherein:

a said data packet having an associated said QoS having a higher value is placed at a position in said transmission queue for transmission ahead of another said data packet having another associated said QoS having a lower value.

4. A method as claimed in claim 2, wherein:

a said data packet containing voice data is placed at a position in said transmission queue for transmission ahead of a said data packet containing streaming media, and said data packet containing steaming media is placed at a position in said transmission queue for transmission ahead of a said data packet containing non-voice data or non-streaming media data.

- 32 -

5. A method as claimed in claim 1, wherein:

the length between said periods of time is less for a said data packet having an associated said QoS having a higher value than a said data packet having another associated said QoS having a lower value.

6. A method as claimed in claim 1, further comprising:

monitoring a duration of time beginning when said attempt to transmit occurs;  
and

repeating said step of controlling said attempt to retransmit at said periods of time until said duration of time exceeds a desired duration of time for said QoS associated with said packet.

7. A method as claimed in claim 6, further comprising:

discarding said packet when said duration of time exceeds said desired duration of time for said QoS associated with said packet.

8. A method as claimed in claim 6, wherein:

the length of said duration of time decreases as a magnitude of said QoS associated with said packet increases.

9. A method as claimed in claim 6, wherein:

the length of said duration of time for a said data packet containing voice data is less than the length of said duration of time for a said data packet containing streaming media, and the length of said duration of time for a said data packet containing streaming media is less than the length of said duration of time for a said data packet containing non-voice data or non-streaming media data.

10. A method for controlling a node in a wireless ad-hoc communication network to identify the presence of other nodes in the network, comprising:

- 33 -

controlling said node to transmit at least one message to be received by those of said other nodes within a broadcast range of said node;

controlling said node to receive responses to said at least one message transmitted by said those of said other nodes; and

determining respective identities of said those of said other nodes relative to said node, and at least one route for said node to communicate with another network, based on said responses.

11. A method as claimed in claim 10, wherein:

said determining determines said respective identities of said those of said other nodes based on respective power levels at which said node receives said respective responses.

12. A method as claimed in claim 10, wherein:

said determining further includes determining respective locations of said those of said other nodes based on said respective responses.

13. A method as claimed in claim 10, wherein:

at least one of said messages transmitted by said node includes information pertaining to a location of said node and an indication of the suitability of said node to act as a position reference.

14. A method for routing at least one data packet between a source node and a destination node in a mobile ad-hoc routing network comprising a plurality of nodes, the method comprising:

determining at least one routing path for routing said data packet between said source node and said destination node based on an amount of energy allowed to be expended by said source node to transmit said data packet, a number of other said nodes permitted as hops between said source node and said destination node, an amount of data congestion in an area of said network including said source and

- 34 -

destination nodes, and an amount of power remaining in a power source of said source node; and

controlling said source node to transmit said data packet to said destination node along said determined routing path.

15. A method as claimed in claim 14, wherein:

said determining step determines a plurality of said routing paths available for routing said data packet between said source node to said destination node.

16. A method for determining at least one route for routing at least one data packet between a source node and a destination node in a mobile ad-hoc communication network comprising a plurality of nodes, the method comprising:

identifying those of said nodes that said source node can use to route said data packet to said destination node based on respective characteristics of said respective nodes;

including said those of said nodes in a group of available nodes; and

determining a route including at least one of said available nodes identified in said identifying step for routing said data packet from said source node to said destination node.

17. A method as claimed in claim 16, further comprising:

removing at least one of said nodes from said group of available nodes based on a change in characteristics of said at least one of said nodes, or a change in position of said source node, or both.

18. A method as claimed in claim 16, wherein each said respective characteristic associated with each respective node includes as indication as to whether said respective node is at least one of the following types of nodes:

an access node capable of providing said source node access to another network or another portion of said network;

- 35 -

a neighboring node of said source node;  
a neighbor of at least one neighboring node of said source node;  
a terminal node which is actively a source or sink of data traffic; and  
a wireless router which is not a neighboring node of said source node.

19. A method as claimed in claim 18, wherein said including includes a node in said group of available nodes based on the following priority:

an access node having the highest priority, followed by a neighboring node, a neighbor of said neighboring node, a terminal node, and a wireless routing having the lowest priority.

20. A method as claimed in claim 18, further comprising:

removing at least one of said nodes based on the following priority:

an access node having the lowest priority for removal, followed by a neighboring node, a neighbor of said neighboring node, a terminal node, and a wireless routing having the highest priority for removal.

21. A method as claimed in claim 16, further comprising:

determining a respective characteristic of a respective said node based on at least one message received by said source node from said respective said node.

22. A method as claimed in claim 21, wherein:

said message includes information pertaining to the power and data rates of connections between nodes neighboring said source node and other nodes.

23. A method for enabling a node in a wireless ad-hoc communication network to identify an access node via which said node is able to access another network or another portion of said network, the method comprising:

- 36 -

controlling said node to send a message to other nodes in said network, said message including a request for identification of a said access node with which said node is associated; and

identifying a certain said access node as being associated with said node based on information contained in a response message received by said node from said access node.

24. A method as claimed in claim 23, wherein:

said node receives said response message that was routed from said access node through at least one of said other nodes.

25. A method as claimed in claim 23, further comprising:

controlling said node to send at least one data packet to said access node via at least one of said other nodes.

26. A method as claimed in claim 25, wherein:

said controlling step controls said node to send said at least one data packet to said access node as a unicast message.

1/7

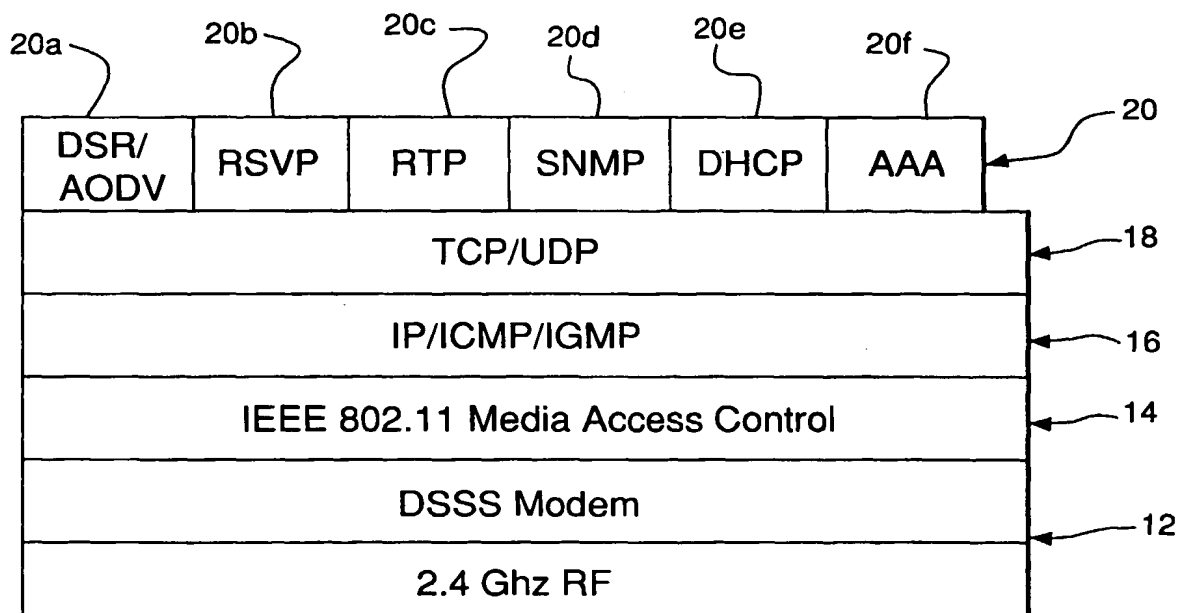


Figure 1

2/7

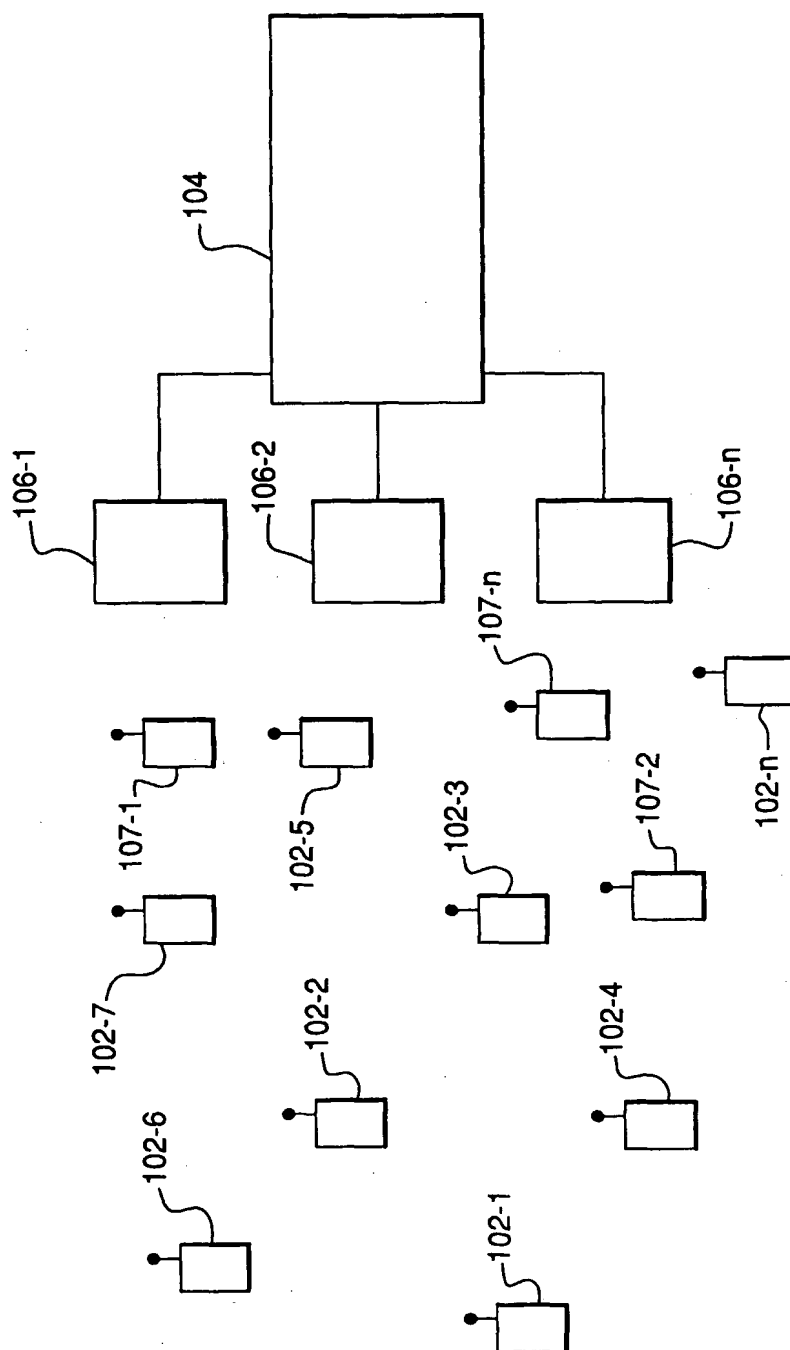


Figure 2



3/7

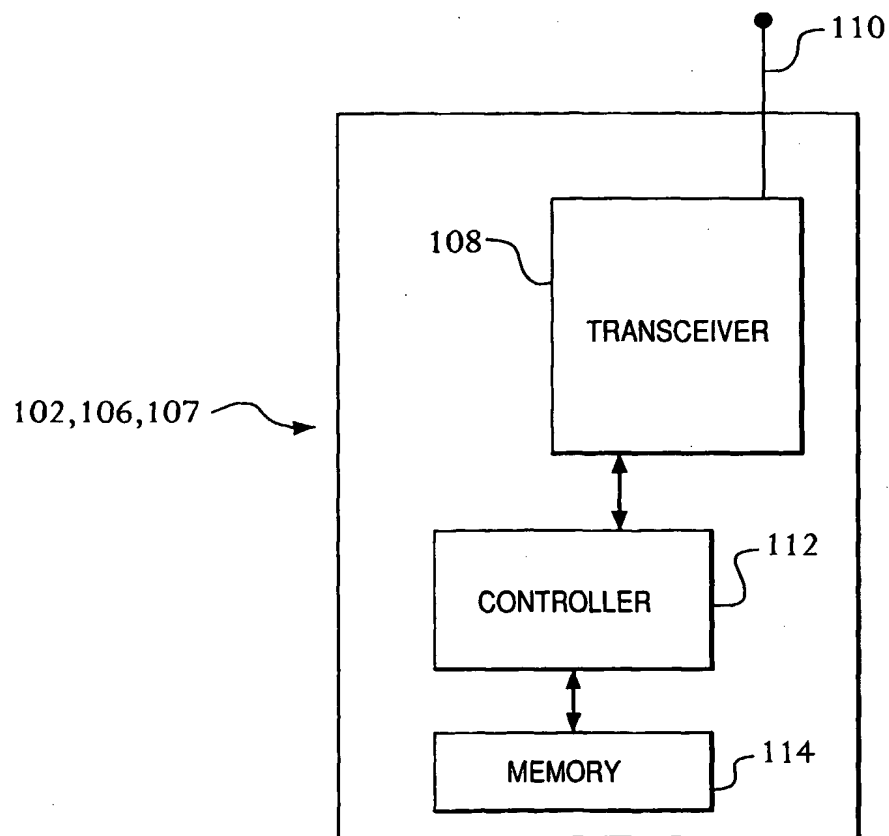


Figure 3

4/7

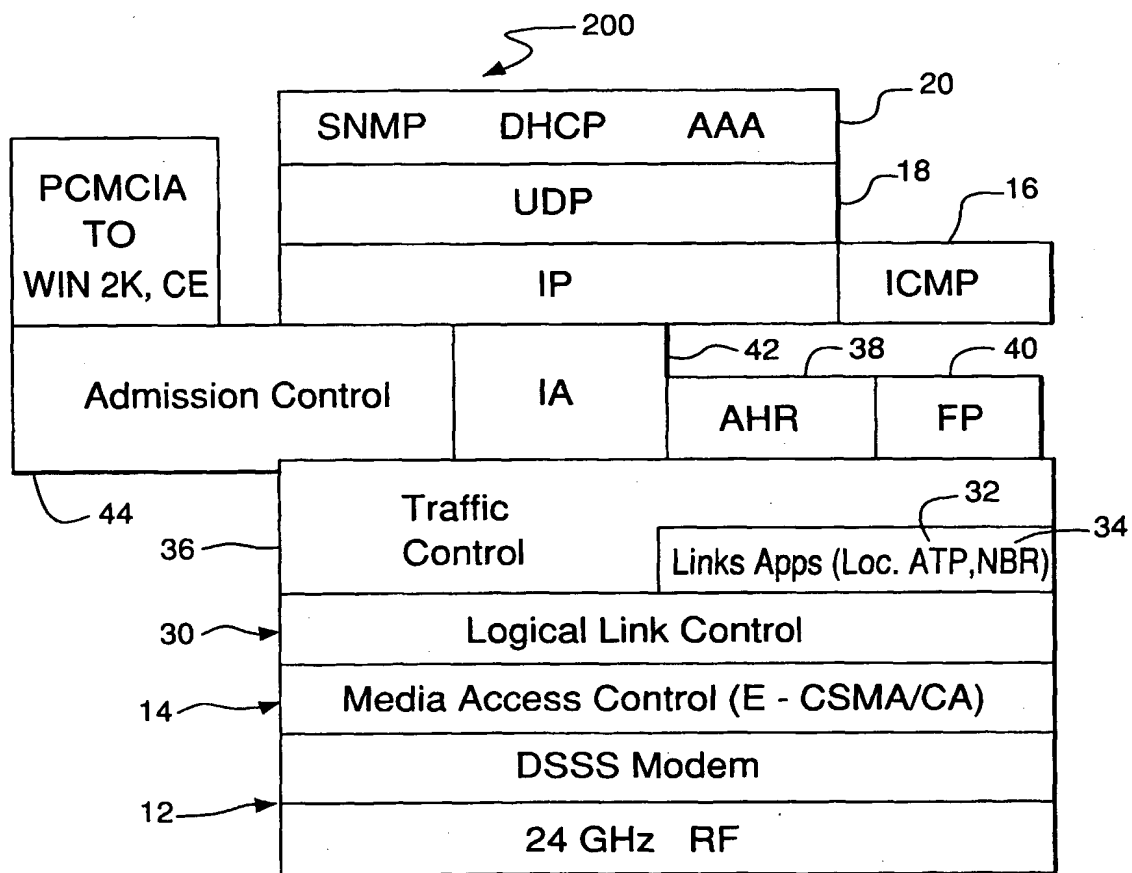
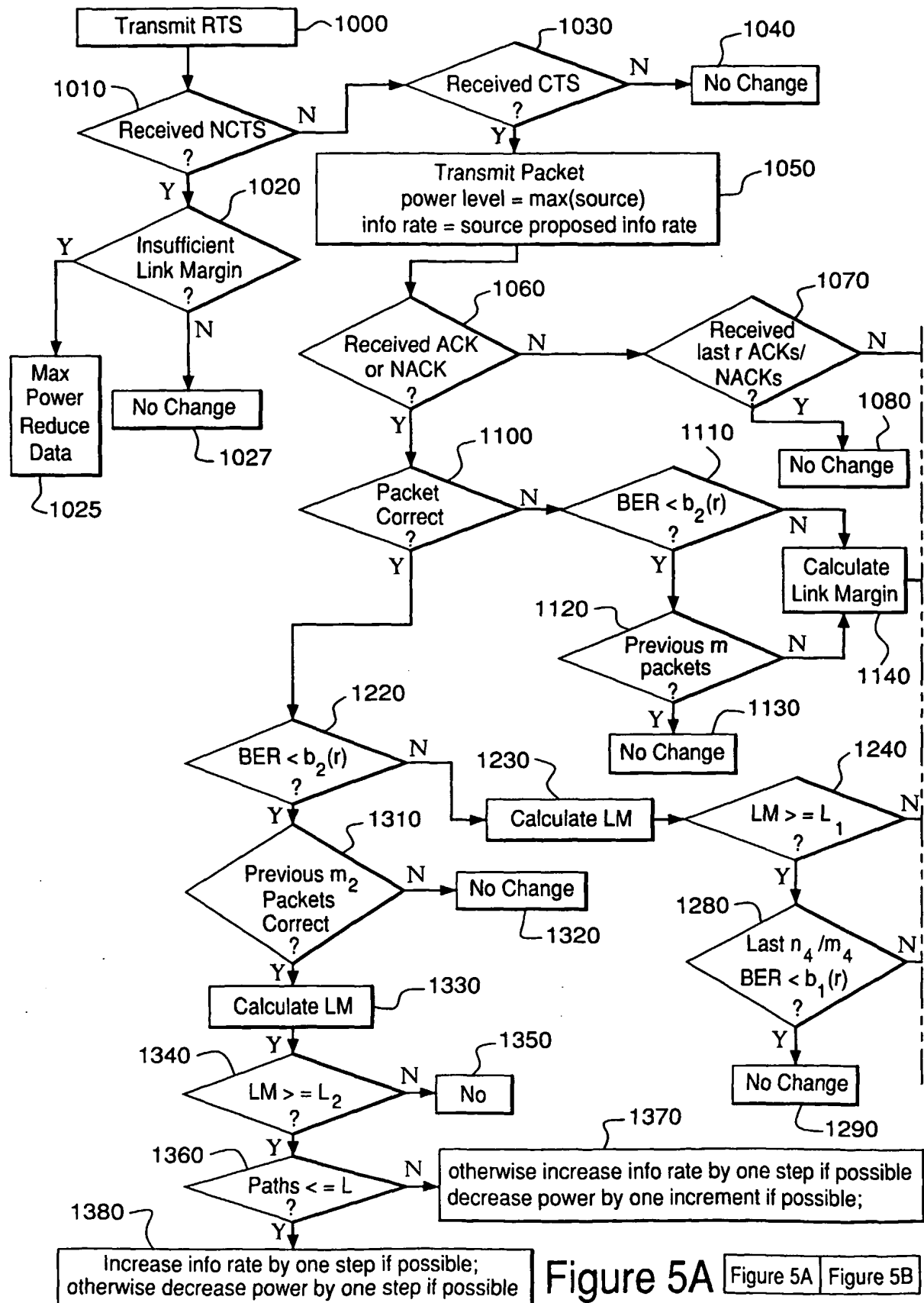


Figure 4

5/7



6/7

LM = Link Margin

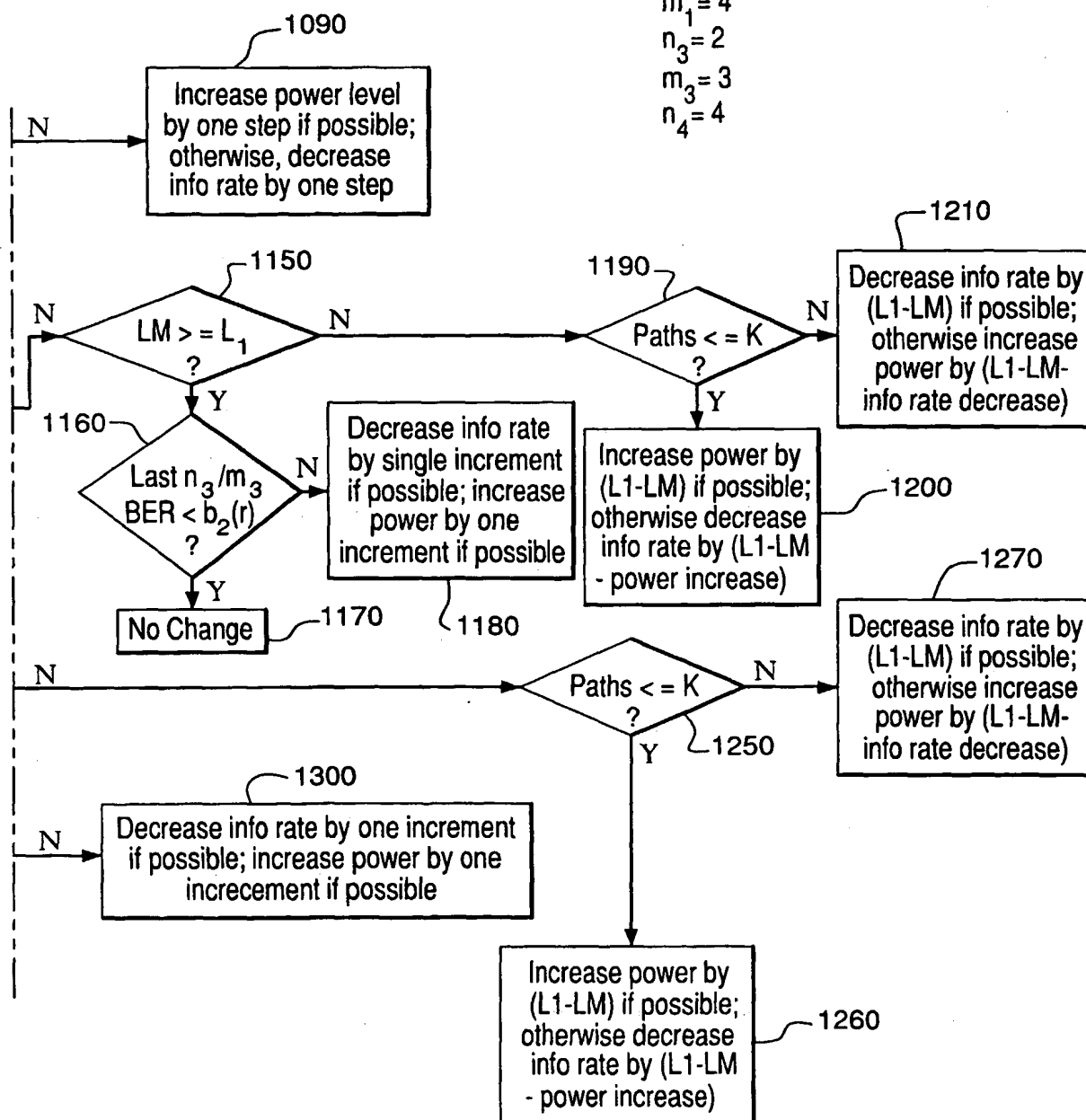
 $L_1$  = Increasing Energy Link Margin $L_2$  = Decreasing Energy Link Margin $B_1(r) = E-2$  $B_2(r) = E-3$  $m_1 = 2$  $m_1 = 4$  $n_3 = 2$  $m_3 = 3$  $n_4 = 4$ 

Figure 5B

7/7

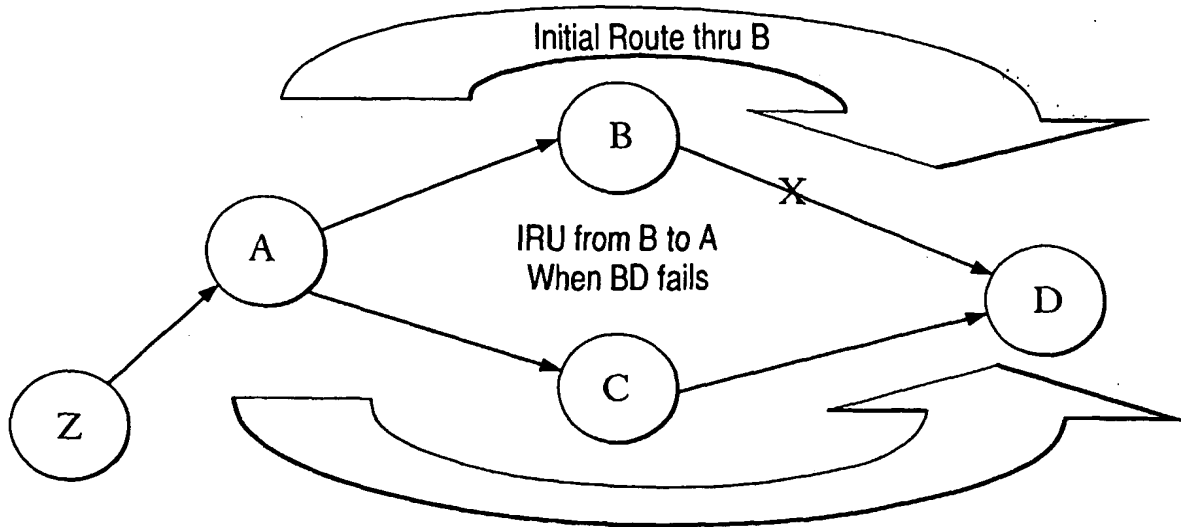


Figure 6

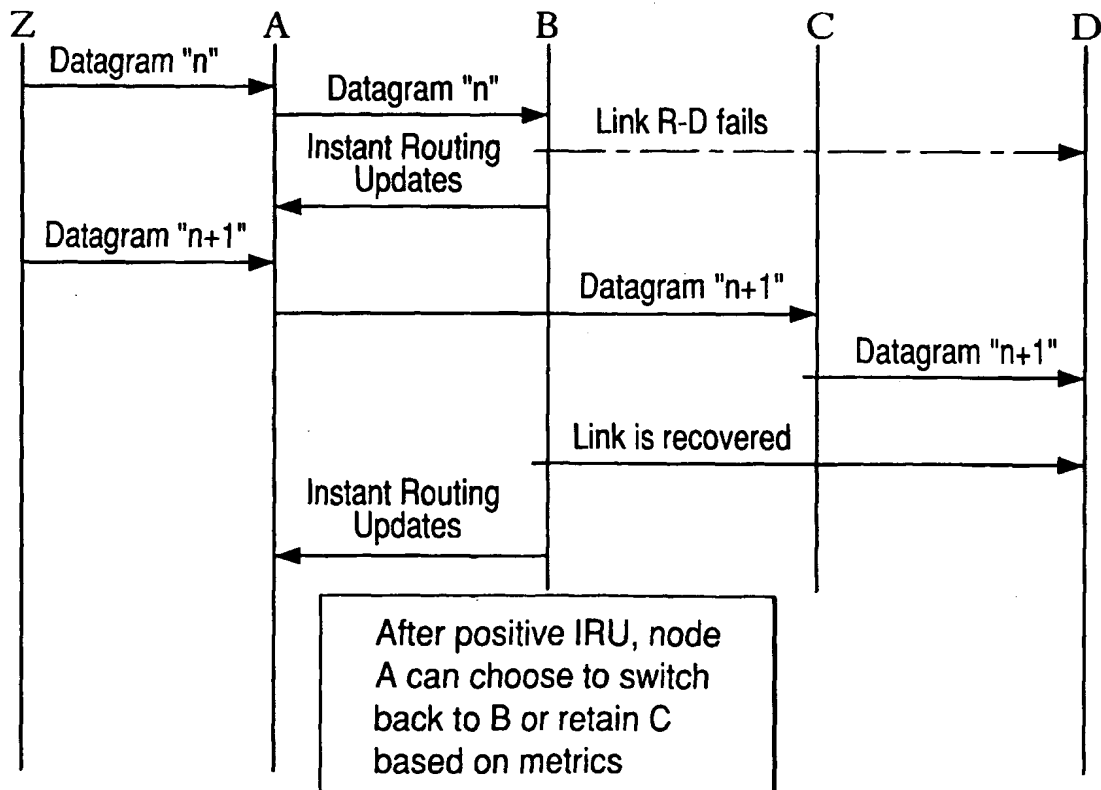


Figure 7

**THIS PAGE BLANK (USPTO)**

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
27 December 2002 (27.12.2002)

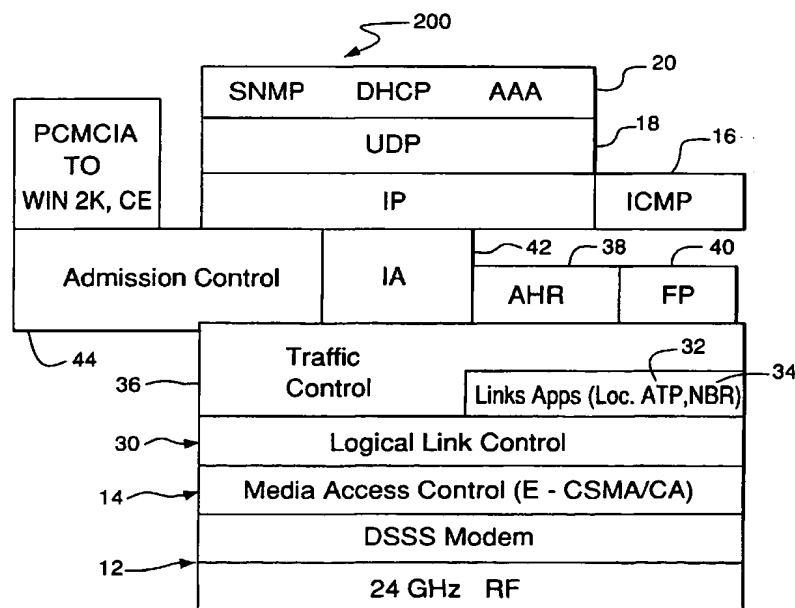
PCT

(10) International Publication Number  
**WO 02/103610 A3**

- (51) International Patent Classification<sup>7</sup>: **G01R 31/08**, G06F 11/00, H04B 7/00, 7/005, 1/44
- (74) Agents: **BU CZYNSKI, Joseph et al.**; Roylance, Abrams, Berdo & Goodman, L.L.P., 1300 19th Street, N.W., Suite 600, Washington, DC 20036 (US).
- (21) International Application Number: PCT/US02/16855
- (22) International Filing Date: 31 May 2002 (31.05.2002)
- (81) Designated States (*national*): AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 60/297,769 14 June 2001 (14.06.2001) US
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- (71) Applicant (*for all designated States except US*): **MESH-NETWORKS, INC.** [US/US]; 485 North Keller Road, Suite 250, Maitland, FL 32751 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (*for US only*): **WHITEHILL, Eric** [US/US]; 6021 Highgate Place, Fort Wayne, IN 46815 (US). **WHITE, Eric** [US/US]; 834 Grant Regency Pointe, Apt. 4-105, Alamonte Springs, FL 32714 (US).

[Continued on next page]

(54) Title: ROUTING ALGORITHMS IN A MOBILE AD-HOC NETWORK



(57) Abstract: A novel software architecture protocol stack with embedded routing algorithms under the Internet Protocol (IP) routing layer in order to provide high quality distribution of multimedia (voice, video, and data) services. These routing algorithms may include logical link control (30), adaptive transmission protocol, neighbor discovery, traffic control (36), Ad-hoc routing, flow processing, intelligent access and admission control (44). These routing algorithms when implemented further provide for advantages in speed of service, reliability of service, self-healing in case of catastrophic failure of an infrastructure component, load-balancing and geographic reuse.



**Published:**

— with international search report

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

**(88) Date of publication of the international search report:**

3 July 2003



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/16855

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G01R 31/08; G06F 11/00; H04B 7/00, 7/005, 1/44.  
US CL : 370/277, 278, 282, 235.

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
U.S. : 370/277, 278, 282, 235.

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
EAST, AD-HOC

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 6,370,375 B (SHIVELY) 09 April 2002 (09.04.2002), column 5 lines 15-40, figure 1.	1-26
X,P	US 6,338,087 B (OKANOUE) 08 January 2002 (08.01.2002), figures 1 and 2, column 11, lines 5-30.	1-26
X,P	US 6,304,556 B (HAAS) 16 October 2001 (16.10.2001), column 7, lines 10-55, column 8, lines 40-65, figure 1.	1-26

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:	
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier application or patent published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

26 September 2002 (26.09.2002)

Date of mailing of the international search report

07 FEB 2003

Name and mailing address of the ISA/US

Commissioner of Patents and Trademarks  
Box PCT  
Washington, D.C. 20231

Facsimile No. (703)305-3230

Authorized officer

*Thien D Tran*  
Thien D Tran

Telephone No. (703) 308-4388

**THIS PAGE BLANK (USPTO)**